DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
9301 CHAPEK ROAD
FORT BELVOIR, VA 22060-5527

REPLY TO
ATTENTION OF

05-27-AMCIO-P

AMCIO-P 22 May 2005

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Materiel Command (AMC) Secure Communications Initiatives

1. References:

a. ALARACT Message, Vice Chief of Staff, Army (VCSA), 16 August 2004, subject: Chief of Staff of the Army (CSA) Conference Guidance-immediate and Near Term Information Assurance (IA) Actions.

b. Memorandum, NETC-EST-A, 01 October 04, subject: Blackberry Common Access Card (CAC) Sled Procurement Guidance.

c. AMC Policy Memorandum 380-24, AMCIO-P, 30 January 2004, subject: Subject: CAC/Public Key Infrastructure (PKI) Guidance for the Use of Digital Signature and Encryption.

d. Memorandum, AMCIO-P, 14 January 2005, subject: AMC Principal Staff Secure Communications.

2. Over the course of the past few months, increased emphasis has been put on Army leadership to improve security of communication by making better use of the technologies that are currently available. Paragraphs 3-6 below outline my secure communications initiatives and direct all AMC Commanders to ensure execution of the associated actions immediately.

3. All AMC Senior Leadership (e.g., General Officers (GO) and Senior Executive Service (SES) personnel and principal staff) must digitally sign and encrypt e-mail correspondence exchanged between one another over the Non-secure Internet Protocol Router Network (NIPRNET). This requirement includes e-mail communication exchanged via handheld wireless devices. For all other personnel, e-mail will be digitally signed if it is considered official business and/or Sensitive Information and encrypted when it is necessary to ensure the confidentiality of information that is sensitive, protected by the Privacy Act, or protected under the Health Insurance Portability and Accountability Act (HIPAA).

4. E-mail traffic containing operational data shall he sent via the Secure Internet Protocol Router Network (SIPRNET). Further, it is a requirement at AMC that all Commanders be equipped with SIPRNET on their desktop to facilitate access to the secure network.

AMCIO-P
SUBJECT: U.S. Army Materiel Command (AMC) Secure Communications Initiatives

5. To ensure continuity of communication for senior leadership, all Flag Officers must have access to their own "Mobile Office." Mobile Office includes a CAC-enabled laptop with mobile networking technology, a CAC-enabled Blackberry, and emergency telecommunications capabilities provided by the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs.

6. Finally, all AMC GOs and SESs must recover their PKI encryption certificates. The reason for this is twofold. First, all personnel will be required to renew their CACs when the cards expire. It is important that these senior leaders be able to read and retrieve e-mail that has been encrypted with their expired keys, and key recovery facilitates this. Second, having a backup copy of the encryption key allows our leaders to have access to their encrypted e-mail should their CAC be unavailable for any reason (e.g., lost or damaged).

7. Any questions or concerns should be referred to G-6, Strategic Planning and Technical Implementation Division, DSN 656-8824, 703-806-8824, DSN 656-8660, or 703-806-8660.

//Signed//
BENJAMIN S. GRIFFIN
General, USA
Commanding